IN THE SPECIFICATION:

In the Background of the Invention, page 3, the paragraph beginning at line 23, has been rewritten as follows:

--It is possible to perform provisioning using short message service (SMS) messages. It is possible to enhance the security of these provisioning messages by means of PIN codes, or secrets in the phone. It is also possible to utilize a public key infrastructure (PKI) ~~infrastructure~~ and signing to enhance security. However, using the default characteristics of a GPRS network, and the chain of trust that can be derived from this environment is not addressed by the prior art.--

In the Summary of the Invention, at page 9, the sub-paragraph beginning at line 26, has been rewritten as follows:

-- • The present invention moves the focus of Data Services rollout from settings management to ~~data~~ Data Service Management. It allows the industry to copy the success of short message service (SMS) messaging to the data space.--

In the Disclosure of Invention and Best Mode for Carrying Out the Invention, at page 18, the paragraph beginning at line 7, has been rewritten as follows:

-- Before providing said provisioning signal **38,** the authentication process takes place. The security of configuring the terminal **10** from a terminal **10** point of view is ensured by means of a chain of trust built using the trusted HLR **18** (or trusted visitor location register (VLR) if access point roaming is permitted)**,** the well-known APN for accessing the trusted access point node **20,** ~~the trusted APN 20,~~ the trusted DNS server **22** and the well-known URL string.--

At page 18, the paragraph beginning at line 13, has been rewritten as follows:

-- The next step is to authenticate the terminal **10** from the network **16** point of view. The authentication mechanism may rely on a pure network authentication (based on MSISDN), and/or may use a send-SMS-to-client / reply-SMS-by-user mechanism to make the authentication procedure stronger. In most systems the gateway GPRS support node (GGSN) is aware of the mapping between the IP address and the MSISDN or international mobile user identity (IMSI). This is typically communicated to an AAA server (the server program which handles user requests for access to computer resources and for an enterprise, provides authentication, authorization and accounting (AAA) services) by means of a Radius protocol. Associated with this Radius (AAA) server there is typically a database that keeps track of an active IP-address to MSISDN mappings. Thus the help-portal server **24** (or its proxy) must query this database in order to authenticate the ~~use~~ terminal **10**. This is one possible scenario among others for implementation of an authentication block **26** of the network **16** shown in Figure 1.--

At page 18, the paragraph beginning at line 27, has been rewritten as follows:

--The authenticity of the terminal **10** from the network point of view is ensured in the example of Figure 1, according to the present invention, by the verification process executed by the help-portal server **24**. A user authentication request signals **32a** and/or **32b** are sent to the authentication block **26** of the network **16** and/or to the terminal **10** by the help-portal server **24**, which receives back ~~an~~ authentication confirmation signals **34a** and/or **34b** from the authentication block **26** and/or from the terminal **10**, respectively. The determination if the user is authentic is made by the help-portal server **24** based on the authentication confirmation signals **34a** and/or **34b**, respectively.--

On page 22, the paragraph beginning at line 13, has been rewritten as follows:

-- In a next step **53**, the help-portal server **24** sends the user authentication request signals **32a** and/or **32b** to the authentication block **26** of the network **16** and/or to the terminal **10** and receives back ~~an~~ the authentication confirmation signals **34a** and/or **34b** from the authentication block **26** and/or from the terminal **10**, respectively.--

On page 23, the paragraph beginning at line 3, has been rewritten as follows:

-- The flow chart of Figure 4 only represents one possible scenario among many others. In a method according to the present invention, in a first step **40a**, the user **14** starts the browser user agent block **12** of the terminal **10** by sending the starting signal ~~**31**~~ **31a**. In a next step **42a**, the browser user agent block **12** sends the access-request signal **30a** (typically containing the well-known URL string for the help-portal server **24** and for the device management server **28a**, the user identification, and the well-known APN name or a wildcard APN as described above) to the network **16** for connecting to the help-portal server **24a** of said network **16** and for requesting the management session signal **38a** for configuring the terminal **10**.--

On page 23, the paragraph beginning at line 24, has been rewritten as follows:

-- In a next step ~~**53**~~ **53a**, the help-portal server ~~**24**~~ **24a** sends the user authentication request signals **32a** and/or **32b** to the authentication block **26** of the network **16** and/or to the terminal **10** and receives back ~~an~~ the authentication confirmation signals **34a** and/or **34b** from the authentication block **26** and/or from the terminal **10**, respectively.--